

# Innovative uses as a result of DNSSEC

Jay Daley .nz



# Disclaimer

- ☞ This is highly opinionated
- ☞ I may be wrong

# Spreading usage

- ④ ADDRESS MAPPING - where do I connect?
- ④ SECURITY - how do I connect?
  - ④ Current RRs (e.g. SSHFP) unused
  - ④ DANE will change this
- ④ POLICY - should I connect?
  - ④ Growth area
  - ④ Squeeze policy into one line! - madness

# Bifurcation

- ☞ Useful generic characteristics of DNS
  - ☞ By design: Scalable, distributed, route around failure, compact, replicating, SECURE
  - ☞ By accident: Firewall transparent, high investment
- ☞ So seems natural for databases
  - ☞ More clever database features needed
    - ☞ Pointers, indexes etc
  - ☞ But - loose synchronisation under threat

# Peer 2 Peer DNS

- ⌚ Threat from asymmetry of attack bandwidth vs defense bandwidth - DDoS
- ⌚ P2P natural mitigation
- ⌚ P2P is all about trust
- ⌚ DNSSEC provides trust for data integrity
- ⌚ BUT still no trust for server integrity
  - ⌚ Not hard to solve!
- ⌚ AND high performance not trivial

# Side effects

- ☞ Crypto in Enterprise now common
- ☞ DNSSEC another crypto function
  - ☞ Good examples of management processes
    - ☞ e.g. Split of KSK, ZSK
- ☞ Clear now - Enterprises need CA function
  - ☞ Following that best practice
    - ☞ Organisational root keys
    - ☞ Translate keys between different formats (hard)

# Any questions?

[jay@nzrs.net.nz](mailto:jay@nzrs.net.nz)

